OIPE IAP45
MAY 24 2006
PATENT & TRADEMARK OFFICE



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | |
|---|---|
| In re application of: | |
| Michael E. Graves, *et al.* | Art Unit: 3621 |
| Serial No: 09/818,084 | |
| Filed: March 26, 2001 | Examiner: Jalatee Worjloh |
| For: AUTHENTICATED PAYMENT | |

**TRANSMITTAL OF APPEAL BRIEF**

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

**ATTENTION: Board of Patent Appeals and Interferences**

Sir:

Attached hereto is Appellants' Brief for the above-referenced application. The Commissioner is authorized to charge the requisite fee $500.00 (37 CFR 1.17(c) and all other fees associated with this submission, to Deposit Account No. 11-0600.

Respectfully submitted,

Date: May 24, 2006

David J. Zibelli
Registration No. 36,394

KENYON & KENYON LLP
1500 K Street, N.W. - Suite 700
Washington, D.C. 20005-1257
Tel: (202) 220-4200
Fax: (202) 220-4201
612246


IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | |
|---|---|
| In re application of: | |
| Michael E. GRAVES, *et al* | Examiner: Jalatee WORJLOH |
| Serial No: 09/818,084 | |
| Filed: March 26, 2001 | Art Unit: 2846 |
| For: AUTHENTICATED PAYMENT | |

APPEAL BRIEF UNDER 37 CFR 41.37

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

**ATTENTION: Board of Patent Appeals and Interferences**

Sir:

Applicants submit this Appeal Brief in the above-referenced application. A Notice of Appeal was filed on January 24, 2006.

## REAL PARTY IN INTEREST

Verisign, Inc. is the real party in interest for all issues related to this application by virtue of an assignment recorded at Reel 011643, Frame 0626.

## RELATED APPEALS OR INTERFERENCES

There are no other appeals, interferences, or judicial proceedings known to Appellants, appellants' legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

05/25/2006 SZEWDIE1 00000157 09818084
01 FC:1252 450.00 DA
05/25/2006 SZEWDIE1 00000157 09818084
02 FC:1402 500.00 DA

## STATUS OF CLAIMS

This application contains claims 1-55. Claims 1-34 have been canceled. Claims 35-55 stand finally rejected as obvious over prior art and are the subject of this appeal.

## STATUS OF AMENDMENTS

No Amendments After Final Rejection were filed in this application.

## SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 35 recites a method for authenticating a payment transaction over a network (authenticate payment instrument, page 4, lines 23-25, authentication request 330, page 17, lines 20-22, network such as Internet, page 15, lines 8-18) storing a public key associated with a public key infrastructure (PKI) key pair in a profile database (public key stored in profile database 150, page 15, line 26-page 16, line 1, Figs. 1 and 3), in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller (page 17, lines 20-22, authentication request 330), sending a challenge request to the buyer over the network (challenge request 240, 340 sent to buyer, page 12, lines 21-22, page 17, lines 24-26), the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer using a private key associated with the PKI key pair (page 17, lines 25-26, summary of payment displayed to buyer, Figs. 6 and 7, page 18, line 18-page 19, line 5), in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally signed summary of the payment transaction, determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed summary of the payment transaction (page 18, lines 1-4); if so determined, storing a digitally signed record of the payment transaction in a transaction archive (transaction archive 170, page 14, line 23-page 15, line 2); and

(page 23, line 21-page 24, line 3); sending an authentication response to the seller over the network (page 13, lines 14-16).

Independent claim 42 recites a computer readable medium storing instructions adapted to be executed by a processor (authentication service 130 inherently includes processor that can store instructions), the instructions including a method for authenticating a payment transaction over a network (authenticate payment instrument, page 4, lines 23-25, authentication request 330, page 17, lines 20-22, network such as Internet, page 15, lines 8-18), the method comprising storing a public key associated with a public key infrastructure (PKI) key pair in a profile database (public key stored in profile database 150, page 15, line 26-page 16, line 1, Figs. 1 and 3); in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller (page 17, lines 20-22, authentication request 330), sending a challenge request to the buyer over the network (challenge request 240, 340 sent to buyer, page 12, lines 21-22, page 17, lines 24-26), the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer using a private key associated with the PKI key pair (page 17, lines 25-26, summary of payment displayed to buyer, Figs. 6 and 7, page 18, line 18-page 19, line 5); in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally signed summary of the payment transaction, determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed summary of the payment transaction (page 18, lines 1-4); if so determined, storing a digitally signed record of the payment transaction in a transaction archive (transaction archive 170, page 14, line 23-page 15, line 2); and (page 23, line 21-page 24, line 3); and sending an authentication response to the seller over the network. (page 13, lines 14-16).

Independent claim 49 recites a system (100, pages 7-8) for authenticating a payment transaction over a network, comprising: a profile database (150); a transaction archive (170); and an authentication service web server (130) coupled to the profile database, the transaction archive and the network, the authentication service web server adaptively configured to: store a public key associated with a public key infrastructure (PKI) key pair in a profile database (public key stored in profile database 150, page 15, line 26-page 16, line 1, Figs. 1 and 3); in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller (page 17, lines 20-22, authentication request 330), send a challenge request to the buyer over the network (challenge request 240, 340 sent to buyer, page 12, lines 21-22, page 17, lines 24-26), the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer using a private key associated with the PKI key pair (page 17, lines 25-26, summary of payment displayed to buyer, Figs. 6 and 7, page 18, line 18-page 19, line 5); in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally signed summary of the payment transaction, determine whether the buyer has access to the private key by using the public key to decrypt the digitally signed summary of the payment transaction (page 18, lines 1-4); if so determined, store a digitally signed record of the payment transaction in a transaction archive (transaction archive 170, page 14, line 23-page 15, line 2); and (page 23, line 21-page 24, line 3); and send an authentication response to the seller over the network (page 13, lines 14-16).

## GROUNDS OF REJECTION TO BE REVIEWED

The July 26, 2005 Final Rejection rejects claims 35, 37-42, 44-49 and 51-55 under 35 U.S.C. §103 over Gifford (US Pat. 6,205,437) in view of Bishop (US Pat. Pub. 2004/0243520) and Shwartz (US Pat. Pub. 2001/0044787), and rejects claims 36, 43

and 50 under 35 U.S.C. §103 over Gifford, Bishop and Schwartz and further in view of Baltzley (US Pat. Pub. 2001/0014158).

## ARGUMENT

The Office Action fails to establish a *prima facie* case of obviousness for any of the claims on appeal. Details of these arguments are presented below.

### Claims 35, 37-42, 44-49 and 51-55 Are Not Obvious

In rejecting claims under 35 U.S.C. §103, the Examiner bears the initial burden of presenting a *prima facie* case of obviousness. See In re Rijckaert, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993). Further, the Examiner must not only identify the elements in the prior art, but also show some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead the individual to combine the relevant teachings of the references. In re Fine, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). Such evidence is required in order to establish a *prima facie* case of obviousness. In re Piasecki, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787-88 (Fed. Cir. 1984).

In the Final Rejection the Examiner states on page 1 that the Amendment filed on 11/8/05 is sufficient to overcome the Davis reference alone, and then proceeds to reject all pending claims over Davis in view of Barnett. On page 2, the Examiner asserts that Davis discloses a smart card that may be programmed with various types of functionality, such as a stored value application; credit/debit; loyalty programs, etc, citing to col. 3, lines 40-50. The Examiner interprets these disclosures as receiving a purchase offer, including a data subject identifier, a data recipient identifier and a price from a data subject...sending a list of stored accepted stored value instruments...

It is unclear what part of the independent claims the Examiner considers to be missing from Davis. There does not appear to be a reference by the Examiner to Barnett until page 25 of the Office Action, where the Examiner indicates that Davis does

not explicitly disclose the user utilizing electronic coupons, and asserts that Barnett discloses the purchasing and online purchasing and electronic coupons. The Office Action further asserts that Barnett discloses sending a list of stored value instruments accepted by the data recipient to the data subject to allow the data subject to choose from the list, and that it would have been obvious to add Barnett's purchasing and user selected coupons to Davis's user being offered discounts or benefits toward purchasing. The Examiner is apparently conceding that Davis does not disclose or suggest sending a list of stored value instruments accepted by the data recipient to the data subject as required by the claims on appeal, which has been Appellant's position throughout.

The Examiner thus acknowledges that Gifford does not disclose sending a challenge request to the buyer over the network, but asserts that in view of the disclosures of Bishop and Shwartz, one of ordinary skill in the art would have been motivated "to modify the method disclosed by Gifford to include the steps of sending a challenge request to the buyer over the network ... because it protects the network server from attacks and improve[s] the ease and safety of electronic commerce for consumers."

In Gifford, a client computer requests a purchase by constructing "a payment order," adding an authenticator, and sending it for approval to a payment computer (*e.g.*, Gifford col. 8, lines 25-28). A payment order describes the identity of a sender, a payment amount, a beneficiary, and a sender unique nonce (Gifford col. 2, lines 59-61). A sender unique nonce is an identifier that is used only once by a given sender (Gifford col. 2, lines 63-64). An example of sender unique nonces are unique timestamps (Gifford col. 2, lines 64-65). A public-key cryptographic signature is used as the authenticator (*see* Gifford col. 10, lines 30-42). The payment order is verified by using the public key known to the payment computer (*see* Gifford col. 8, lines 28-31; col. 10, lines 40-42). Replay attacks are prevented by checking to make sure the sender did not previously send a payment order with the same nonce. (Gifford, col. 8, lines 55-65).

In comparison, the purpose of crytographic challenge in Bishop is to prevent replay attacks (Bishop, para. 0087: "Cryptographic challenge 1004 is any sort of challenge message that prevents replay attacks ... such as a challenge that is based upon random data and is designed to solicit a response from the X. 509 application stored on smartcard 202."; *see also* Bishop, para. 0094: "Authentication server 306 ... then formats a challenge message 1106 (which may include random data)...").

The express purpose of the challenge response in Bishop is to solve the problem of replay attacks, which was already solved by the invention of Gifford. Gifford solves this problem by including a nonce in a payment order which is checked to make sure the sender did not previously send a payment order with the same nonce. The Examiner asserts that it would have been obvious to graft the challenge message feature of Bishop onto the invention of Gifford, as there is no problem to solve. Gifford does not require messages sent back to the client computer, which would be require by the modification of Gifford suggested by the Examiner. Thus, the Examiner's modification would make the procedure of Gifford much more complicated by requiring a challenge message be sent to the client computer and a response to be generated. Such would require additional software in the client computer and in the payment computer to generate and process the challenge and response.

Further, the nonce used in Gifford already protects against replay attacks so that one of ordinary skill in the art would not have been motivation to add the challenge and response of Bishop to solve the replay attacks problem already solved by the nonce of Gifford. The Examiner's combination is thus made with impermissible hindsight reconstruction of the claimed invention.

Further, the applied references do not disclose or suggest "the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer..." as required by the claims. The Examiner states "Bishop et al. disclose sending a challenge request to the buyer over the network, the challenge request message to be displayed to the buyer then digitally signed by the buyer..."

(page 4). There is no suggestion that a component of the challenge message is to be displayed to the user and then digitally signed by the buyer. The cryptographic challenge in Bishop is "any sort of challenge message that prevents replay attacks (e.g., fraudulent messages created by re-sending previously sent authentication packets), such as a challenge that is based upon *random data* and is designed to solicit a response from the X.509 application stored on the smartcard 202." (Bishop para. 0087; *see also* para. 0094 "...then formats a challenge message 1106 (which may include random data) ... The resultant signature request block is provided to smartcard 202 via reader 204. Smartcard 202 suitably signs the block and provides a copy of its X.509 certificate, as appropriate."). The only "display" to the user that Bishop discloses in relation to the challenge request is the option that the card reader 204 may interact with customer computer 110 "to prompt the user for a personal identifier, for example a personal identification number (PIN) or other unique identifier, to access the card." (*See* Bishop para. 0089). This does not suggest the display and signing described in the claims.

The Examiner further suggests that Shwartz disclose a challenge request including a summary of the payment transaction, referring to paragraphs 182-184. However, this does not include a disclosure of "the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer..." as required by the claims. There is no disclosure of what is displayed other than "...presents a window on the display 46 of the communication device 12 asking for approval of the transaction and presenting the challenge." Such is not a disclosure of a summary of the payment transaction to be displayed to the buyer.

For at least the above reasons, it is submitted that claims 35, 37-42, 44-49 and 51-55 would not have been obvious over the applied references. Reversal of the rejections is requested.

**Claims 36, 43 and 50 Are Not Obvious**

Claims 36, 43 and 50 depend from claims 35, 42 and 49, which would not have been obvious over the applied references for the reasons explained above. Further, Baltzley does not solve the above-noted deficiencies of the other applied references, and therefore claims 36, 43 and 50 would also not have been obvious over the applied references for the same reasons set forth above. Reversal of the rejections is requested.

## CONCLUSION

Applicants respectfully requests reversal of the rejections of claims 35-55. These claims are allowable over the cited art.

Respectfully submitted,

Date: May 24, 2006

David J. Zibelli
Registration No. 36,394

KENYON & KENYON
1500 K Street, N.W.
Washington, D.C. 20005
Tel: (202) 220-4200
Fax: (202) 220-4201

## CLAIMS APPENDIX

1-34. (Canceled)

35. A method for authenticating a payment transaction over a network, comprising:

storing a public key associated with a public key infrastructure (PKI) key pair in a profile database;

in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller, sending a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer using a private key associated with the PKI key pair;

in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally signed summary of the payment transaction, determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed summary of the payment transaction;

if so determined, storing a digitally signed record of the payment transaction in a transaction archive; and

sending an authentication response to the seller over the network.

36. The method of claim 35, further comprising:

creating the PKI key pair; and

sending the private key to the buyer over the network.

37. The method of claim 35, wherein the record of the payment transaction is digitally signed using the private key.

38. The method of claim 35, wherein the record of the online transaction is digitally signed using a local private key.

39. The method of claim 35, wherein the public key is stored in the form of a digital certificate representing that the public key is tied to the buyer.

40. The method of claim 35, further comprising:

retrieving a buyer profile from the database, the buyer profile including a plurality of payment instruments and a plurality of shipping addresses;

sending the buyer profile to the buyer over the network; and

receiving a selection of one of the plurality of payment instruments and one of the plurality of shipping addresses from the buyer over the network.

41. The method of claim 35, further comprising:

processing the payment transaction via a payment gateway.

42. A computer readable medium storing instructions adapted to be executed by a processor, the instructions including a method for authenticating a payment transaction over a network, the method comprising:

storing a public key associated with a public key infrastructure (PKI) key pair in a profile database;

in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller, sending a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer using a private key associated with the PKI key pair;

in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally signed summary of the payment transaction, determining whether the buyer has access to the private key by using the public key to decrypt the digitally signed summary of the payment transaction;

if so determined, storing a digitally signed record of the payment transaction in a transaction archive; and

sending an authentication response to the seller over the network.

43. The computer readable medium of claim 42, wherein the method further comprises:

creating the PKI key pair; and

sending the private key to the buyer over the network.

44. The computer readable medium of claim 42, wherein the record of the payment transaction is digitally signed using the private key.

45. The computer readable medium of claim 42, wherein the record of the online transaction is digitally signed using a local private key.

46. The computer readable medium of claim 42, wherein the public key is stored in the form of a digital certificate representing that the public key is tied to the buyer.

47. The computer readable medium of claim 42, wherein the method further comprises:

retrieving a buyer profile from the database, the buyer profile including a plurality of payment instruments and a plurality of shipping addresses;

sending the buyer profile to the buyer over the network; and

receiving a selection of one of the plurality of payment instruments and one of the plurality of shipping addresses from the buyer over the network.

48. The computer readable medium of claim 42, wherein the method further comprises:

processing the payment transaction via a payment gateway.

49. A system for authenticating a payment transaction over a network, comprising:

a profile database;

a transaction archive; and

an authentication service web server coupled to the profile database, the transaction archive and the network, the authentication service web server adaptively configured to:

store a public key associated with a public key infrastructure (PKI) key pair in a profile database;

in response to receiving an authentication request from a buyer over a network, the authentication request including a description of the payment transaction and an identity of a seller, send a challenge request to the buyer over the network, the challenge request including a summary of the payment transaction to be displayed to the buyer and then digitally signed by the buyer using a private key associated with the PKI key pair;

in response to receiving a challenge response from the buyer over the network, the challenge response including the digitally signed summary of the payment transaction, determine whether the buyer has access to the private key by using the public key to decrypt the digitally signed summary of the payment transaction;

if so determined, store a digitally signed record of the payment transaction in a transaction archive; and

send an authentication response to the seller over the network.

50. The system of claim 49, wherein the authentication service web server is further adapted to:

create the PKI key pair; and

send the private key to the buyer over the network.

51. The system of claim 49, wherein the record of the payment transaction is digitally signed using the private key.

52. The system of claim 49, wherein the record of the online transaction is digitally signed using a local private key.

53. The system of claim 49, wherein the public key is stored in the form of a digital certificate representing that the public key is tied to the buyer.

54. The system of claim 49, wherein the authentication service web server is further adapted to:

retrieve a buyer profile from the database, the buyer profile including a plurality of payment instruments and a plurality of shipping addresses;

send the buyer profile to the buyer over the network; and

receive a selection of one of the plurality of payment instruments and one of the plurality of shipping addresses from the buyer over the network.

55. The system of claim 49, wherein the authentication service web server is further adapted to:

process the payment transaction via a payment gateway.

## EVIDENCE APPENDIX

No evidence under 37 CFR 1.130, 1.131 or 1.132 was submitted in this application.

## RELATED APPEALS APPENDIX

There are no other appeals, interferences, or judicial proceedings known to Appellants, appellants' legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

PAGE 1/1 * RCVD AT 7/25/2006 3:08:37 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/20 * DNIS:2736714 * CSID:202 220 4201 * DURATION (mm-ss):00-52

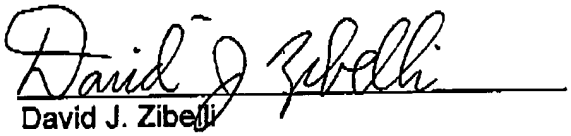


Claims 36, 43 and 50 depend from claims 35, 42 and 49, which would not have been obvious over the applied references for the reasons explained above. Further, Baltzley does not solve the above-noted deficiencies of the other applied references, and therefore claims 36, 43 and 50 would also not have been obvious over the applied references for the same reasons set forth above. Reversal of the rejections is requested.

## CONCLUSION

Applicants respectfully requests reversal of the rejections of claims 35-55. These claims are allowable over the cited art.

Respectfully submitted,



Date: May 24, 2006

David J. Zibelli
Registration No. 36,394

KENYON & KENYON
1500 K Street, N.W.
Washington, D.C. 20005
Tel: (202) 220-4200
Fax: (202) 220-4201



JUL.25'2006 15:09 202 220 4201 KENYON & KENYON #2204 P.001/001